(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 February 2004 (19.02.2004)

PCT

(10) International Publication Number
WO 2004/015917 A1

(51) International Patent Classification[7]: H04L 9/32, G07B 15/02

(21) International Application Number: PCT/FI2003/000597

(22) International Filing Date: 11 August 2003 (11.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20021467 12 August 2002 (12.08.2002) FI

(71) Applicant *(for all designated States except US)*: **OY PLUSDIAL AB** [FI/FI]; Tekniikantie 12, FIN-02150 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **PAKARINEN, Ari** [FI/FI]; Raatimiehenkatu 6 E 74, FIN-00140 Helsinki (FI).

(74) Agent: **BERGGREN OY AB**; P.O. Box 16, Jaakonkatu 3 A, FIN-00101 Helsinki (FI).

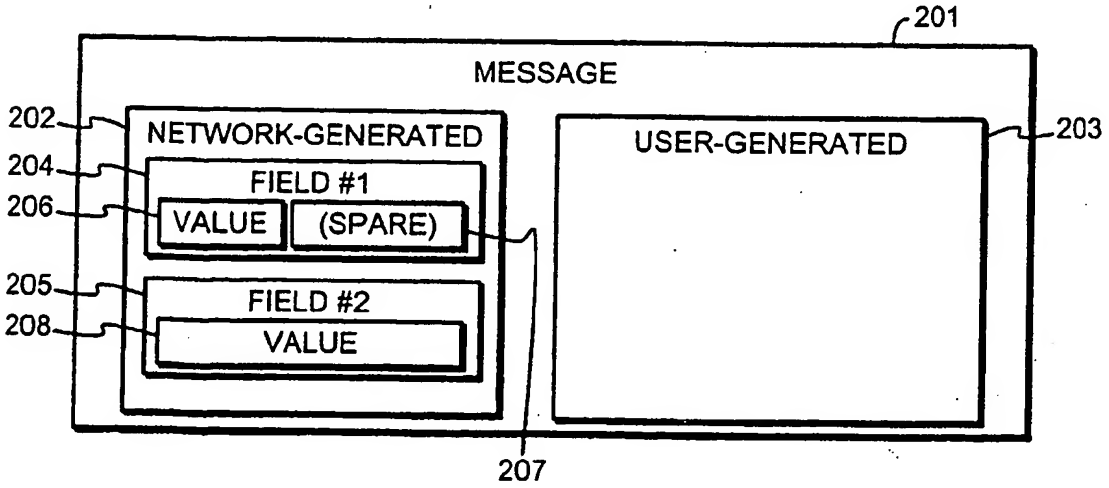
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND ARRANGEMENT FOR AUTHENTICATING A COMMODITY OF VALUE DELIVERED AS A DIGITAL MESSAGE



(57) Abstract: A method and an arrangement are disclosed for authenticat-ing a commodity of value delivered from a closed network as a digital message (201) to a mobile terminal. The digital message (201) has a predefined format that comprises fields (204, 205) for network-generated values (206, 208). Authenticating involves generating (311, 406) a code value according to a time-dependent rule, so that the generated code value depends on the moment of time when the digital message will be transmitted. The generated code value is inserted (311, 406) into a certain first field (204) in the digital message, which first field has a predefined role that is other than conveying code values. Another value that represents message transmission time is inserted (407) into a second field (205) in the digital message.

WO 2004/015917 A1

Method and arrangement for authenticating a commodity of value delivered as a digital message

The invention concerns generally the technology of electronically delivering relatively short and compact messages that represent a commodity of value. Especially the invention concerns the problem of how to ensure that such a message, when presented for inspection, is an authentic one and not an illegal copy.

Electronically delivering various tickets, discount coupons and corresponding commodities of value in the form of SMS messages (Short Message Service), MMS messages (Multimedia Message Service) and similar compact, well-defined messaging formats is rapidly gaining popularity. As an example we may consider the known way of ordering and delivering public transport tickets (such as tram or bus tickets) to the mobile telephones of individual users. In fig. 1 we assume that the user of a mobile telephone 101 wants to order an electronically deliverable bus ticket. The mobile telephone 101 has a wireless communication connection with a base transceiver station 102, from which there is a further connection to a core network 103 of which an SMSC (Short Message Service Center) 104 constitutes a part. A ticket application server 105 is arranged to have a communication connection with the SMSC. Conveying an order message from the mobile telephone 101 through the base transceiver station 102 and the SMSC 104 to the ticket application server 105 is schematically represented in fig. 1 as a series of steps ①, ② and ③. After having received the order message the ticket application server 105 generates an electronic ticket and sends it back to the mobile telephone that ordered it. Conveying a ticket back to the mobile telephone 101 is shown as steps ④, ⑤ and ⑥.

Charging for the electronically delivered ticket is most straightforwardly accomplished by adding a certain fixed price to the telephone bill of the user of the mobile telephone 101. However, after the user has received the ticket message into his mobile telephone, it is usually possible for him to forward a copy of the ticket message to another mobile telephone, like that of a friend who took the same bus. The price for just sending another SMS message is typically considerably lower than the ticket price that was charged of the original recipient of the ticket message. A temptation quickly arises to cheat the system by ordering a single ticket for one of a group of persons and distributing copies of the original ticket as ordinary SMS messages to the other members of the group.

It is of principal importance for the arrangement of fig. 1 to be plausible that it is possible to verify the authenticity of a ticket message at the moment when it is presented for inspection at the user's mobile telephone. A known way of providing authenticity is to rely on the correctness of the sender information that constitutes a part of the ticket message. During the process of conveying an SMS message towards the mobile telephone of a user the network adds the telephone number of the sender to the message. An off-the-shelf mobile telephone does not include any means for forging the sender information in a received SMS message, so an illegally forwarded copy can be recognized by noting that its sender is not the ticket application server.

The reliability of checking the sender is undermined by certain mobile telephone models having a feature that was originally introduced in good faith in order to enhance user-friendliness. The user of the mobile telephone can use a freely selectable alphanumeric string as the identifier of an entry in the directory of stored names and numbers. On the other hand said certain mobile telephone models check the sender's number from a received SMS message, and if the number matches that of a named entry in the directory, they only display the "name" or identifier of that entry as the sender of the message. So if we assume that the telephone number of the ticket application server is 123456 and Tom instructs his mobile telephone to store Eve's number as belonging to somebody named "123456", the following scheme becomes possible: Eve orders and receives an electronic ticket and forwards an illegal copy of it to Tom. When Tom's mobile telephone is inspected, it contains a received SMS message, which the mobile telephone only displays as having been received from "123456". In other words Tom's illegal copy that he received from Eve appears to be an authentic ticket message directly received from the ticket application server.

In general, various approaches are known for authenticating electronically distributed messages. Their drawbacks regarding applicability to the above-described problem usually involve complexity either in required hardware or in resulting message content or both. If a relatively short message must represent a ticket, it should be easy both for ordinary users and for ticket inspectors to perceive it as one. Elaborate alphanumeric code strings in the message tend to raise a suspicion of the system being complicated and difficult to use. Additionally for an inspector to be able to quickly and unambiguously verify the meaning of a complicated code string requires that the inspector carries along an electronic reader and verifier device. The same is true if the message contains some kind of a bar code that the mobile tele-

phone can show on its display, which is one of the suggested message authentication techniques.

A reference publication GB 2 361 570 is known to describe a general-purpose electronic ticket delivery system, in which the ticket is delivered as an SMS message or in a browser-readable format. The SMS solution discussed in said publication is especially prone to the fraud scheme described earlier.

Another known prior art publication is WO 96/06508, which presents a general-purpose method for reliably identifying the originator of an SMS message. The drawback of this scheme is that it requires modifications to the standardised basic operation of conveying SMS messages, because it involves using at least two different addresses in calling a Short Message Services Centre.

It is an objective of the invention to provide a method and an arrangement that ensure easy and reliable authentication of commodities of value that were delivered electronically in the form of digital messages. It is especially an aim of the invention that authentication should require only little, if any, extra investment in system hardware.

The objectives of the invention are achieved by adding a time-dependent extension to the telephone number that the message transmission system includes into the message as the number of the sender.

A method according to the invention has the characteristic features that are recited in the independent patent claim directed to a method.

The invention applies also to an arrangement, the characteristic features of which are recited in the independent patent claim directed to an arrangement.

Various embodiments of the invention are described in the depending claims.

The invention is based on the insight that cheating in the way described above is only possible if the telephone number of the ticket application server is constant, so that the potential cheater can store it beforehand into his mobile telephone (or corresponding mobile telecommunication device) as an identifier of his accomplice. Every time when the telephone number of the ticket application server changes, the cheater must reprogram his mobile telephone. By making the telephone number of

the ticket application server to change very often it is possible to make it difficult or impossible for the cheater to follow. Depending on the number and nature of possible other network-generated field values in a message it may be possible to apply a similar authentication strategy also to other field values than just the sender's telephone number.

According to the invention, there exists a scheme for repeatedly changing an identifier value or identifier values that the network adds into an electronically delivered message. Preferably the scheme utilizes certain spare character locations that have been defined to constitute a part of a field in a transmitted message but are not necessarily needed for the transmission of information when the invention is not applied. Also it is preferable that the changing values are somehow related to another network-generated value in a well-defined field of the message, so that the message becomes self-sustaining regarding verification: for someone who knows the rules according to which the changing values behave, it suffices to compare the contents of the changing-value field to some other field in the message to see whether the message has been appropriately generated and delivered.

The most straightforward candidate for the changing-value field is the field for the sender's telephone number. Typically it comprises relatively many character locations, to reckon with exceptionally long telephone numbers used in certain systems. If the telephone number assigned to a ticket application server is not as long as the maximum length of the sender's number field, the spare character locations can be used to insert a repeatedly changing extension. A simple and workable rule for generating repeatedly changing extensions, that also correlate with the value of another field in the same message, is to utilize as an extension a part of or a derivative from the time value that is inserted into the message as transmission time.

The novel features which are considered as characteristic of the invention are set forth in particular in the appended claims. The invention itself, however, both as to its construction and its method of operation, together with additional objects and advantages thereof, will be best understood from the following description of specific embodiments when read in connection with the accompanying drawings.

Fig. 1 illustrates a prior art setup for electronically ordering and delivering bus ticket messages,

fig. 2 illustrates a principle of using message parts according to the present invention,

fig. 3a illustrates a process of exchanging messages according to an embodiment of the present invention,

fig. 3b illustrates a process of exchanging messages according to another embodiment of the present invention,

fig. 4 illustrates the operation of a ticket application server according to an embodiment of the invention,

fig. 5 illustrates the operation of an intelligent messaging gateway according to an embodiment of the invention and

fig. 6 illustrates certain structural aspects of a ticket application server according to an embodiment of the invention.

The exemplary embodiments of the invention presented in this patent application are not to be interpreted to pose limitations to the applicability of the appended claims. The verb "to comprise" is used in this patent application as an open limitation that does not exclude the existence of also unrecited features. The features recited in depending claims are mutually freely combinable unless otherwise explicitly stated.

Fig. 2 illustrates schematically a message 201, which we may designate as a multimedia message for the sake of generality. Features of the messages that are important to the invention are that it is electronically deliverable from a network to the terminals of individual users and that it has a well-defined and standardized structure that makes it acceptable and usable for an extremely wide population of mobile terminal users. A further feature of the message 201, which is also important to the present invention, is that its standardized composition defines a network-generated part 202 in addition to a user-defined part 203. Considering the widely used SMS message as an example, the network-defined part 202 consists of the parameter values that a network (typically an SMSC) adds to the message, while the user-defined part 203 consists of the (originally maximum of 160) payload characters that a user or a message-generating computer program at a content provider's server puts in.

The network-generated part 202 typically comprises fields, of which fields 204 and 205 are shown in fig. 2, into which the network inserts certain values. We assume that at least one of these fields has a certain maximum length that has been selected to accommodate the longest possible values that can be inserted into that field, with some marginal so that typically the whole length of the field is not needed. As an example we may say that field 204 is a field for the sender's telephone number. Telephone numbers of various lengths appear in different telephone systems around

the world, so the length of the sender's number field 204 must have been selected to accommodate also relatively long telephone numbers. Typically when the present invention is applied, a telephone number that identifies a ticket application server (or other instance that is to generate messages that represent a commodity of value) is shorter than the maximum length of the field 204, so after said telephone number has been inserted as a field value 206, spare space 207 remains in the field 204. Again as an exemplary assumption only we assume that the length of the spare space 207 corresponds to three alphanumeric characters.

Another field 205 also appears in the network-generated part 202 of the message 201. We assume that field 205 is the transmission time field, into which the SMSC should insert a value 208 that represents the moment of time at which the message was originally sent by its sender.

According to a preferable embodiment of the invention, the spare space 207 of the sender number field 204 is used to carry a code, the value of which has a certain relationship to the transmission time value 208 in the appropriate field 205. Taken our exemplary assumption of the spare space 207 being three characters long, an easy option would be to insert a certain fixed character into the spare space 207, followed (or preceded) by a two-digit number that matches the minute count, i.e. the two-digit number that represents minutes, in the transmission time value 208. Another option would be to select said two digits to match the second count in the transmission time value 208. A third option would be to use two digits of the spare space 207 to match the minute count and a third digit to match the number that represents tens of seconds in the transmission time value 208. It is not important to the invention, what is the exact way of mapping the transmission time value into a code value in the spare space 207; the following considerations should anyway be taken into account:

* The mapping algorithm should make the code value to change often enough to make it difficult for a potential cheater to follow. The cheating mechanism explained earlier requires the cheater to store into his mobile telephone a whole new identifier string as the name of his accomplice before forwarding the honestly obtained ticket message. It is reasonable to assume that making the code value change once per minute is enough to curtail at least large-scale cheating.
* The mapping algorithm should be robust against typically occurring time jitter and transitional phenomena in the operation of the network devices. If two different devices or processes are responsible for generating the transmission time value and

the code value, it should be ensured that they synchronize to each other tightly enough so that no contradictory value pairs (that would suggest that cheating had been attempted) are generated at the first place.

* It is advantageous if the mapping algorithm changes, even relativaly slightly, every now and then so that a potential cheater would be confused. For example if the minute count approach is used, there could be a certain fixed offset value that is agreed upon e.g. once a week: this week the two digits in the code match the transmission time minute count plus 11, next week it is the minute count minus 05, and so on. It is easy to understand that the way of changing the algorithm should be kept secret from everybody else than those who have the task of running the system and/or checking the validity of delivered ticket messages.

The message may naturally include also other parts and other fields than just those shown in fig. 2. If there is not enough spare space in one previously determined field and/or if it is considered advantageous for increasing security, code values can also be distributed into more than one field. It is likewise possible to make a single code value depend on more than one other value in more than one other field. In the process of defining a completely new message format it would naturally be possible to define a dedicated code value field for the insertion of a code value; however it is a major advantage of the present invention that the code value is "smuggled" in a previously defined field, moreover so that every ordinary mobile terminal will handle and display the code value in an exactly similar way with absolutely no additional definitions for message handling. The mobile terminals are not even aware of there being any code values involved: they will just handle and display the code value of the present invention as a part of the value that belongs to the appropriate field, which is field 204 in fig. 2.

Fig. 3a illustrates a process of exchanging messages in a system that comprises a mobile terminal, an SMSC that implements the so-called CIMD protocol (Computer Interface to Message Distribution), a messaging gateway and a ticket application. At step 301 the terminal generates a ticket ordering message as a response of a user telling the terminal to do so. At step 302 the terminal transmits the message, and at step 303 the SMSC receives it. Forwarding the message further towards the ticket application may involve certain processing 304 at the SMSC, after which a further transmit/receive step 305 and 306 takes place between the SMSC and the messaging gateway. The latter inspects the incoming message at step 307 enough to find out that it is a ticket ordering message, and passes it further to the ticket application in steps 308 and 309. The ticket application generates the ordered ticket message at

step 310. Up to this point the operation proceeds exactly like in known prior art electronic ticketing applications.

At step 311 the ticket application generates an authentication code that is to be added to the ticket message generated at the previous step. Certain more detailed ways of generating the code will be described later. At step 312 the ticket application transmits the completed ticket message to the messaging gateway, which receives it at step 313 and selects, by using appropriate known methods, the SMSC through which the ticket message should be delivered to the terminal that ordered it.

A feature of the CIMD protocol is that the SMSC does not need to receive a sender's telephone number from the application that generated a message or the gateway that forwarded it to the SMSC: the SMSC has been configured to otherwise know a sender's telephone number that it adds to the message as a part of the process of sending the message towards the terminal. It is possible to provide a sender's telephone number to the SMSC according to CIMD, but the SMSC will still use the configured number and only add the number that came from the application server into the sender's number field after the configured number. In order not to have the same sender's number repeated twice in the message, the messaging gateway – after having recognized the appropriate SMSC as one that implements CIMD – strips off the actual telephone number value from the message at step 315 before sending the message to the SMSC at step 316. The SMSC receives the message at step 317 and executes its conventional processing at step 318: as a part of the last-mentioned it takes the code value that remained in the sender's number field after step 315 and appends it to the end of the sender's number field of the final message. Steps 319 and 320 represent transmitting the ticket message from the SMSC to the mobile terminal in a known way.

Fig. 3b is otherwise the same as fig. 3a, but now we assume that the SMSC implements the so-called Content Gateway interface towards message-generating applications in the network. An important difference to CIMD arrangements is that according to the Content Gateway specifications, the SMSC will not use any configured numbers but will accept and use any sender's number that came with the messsage from an application server. Steps 301 to 314 take place exactly in the same way as in fig. 3a. However, after noticing now at step 314 that the SMSC implements Content Gateway rather than CIMD, the messaging gateway now preserves at step 315' the contents of the sender's number field as they were in the message that came from the ticket application. Step 318' proceeds in the SMSC according to the Con-

tent Gateway specifications, so the SMSC reads the whole contents of the sender's number from the message it received from the messaging gateway at step 317 and reuses it as such in the message it transmits to the mobile terminal at step 319.

Fig. 4 illustrates the operation of a ticket-generating application according to an embodiment of the invention. At step 401 the application receives a ticket order message from an SMSC, typically through a messaging gateway. At step 402 the application extracts the sender's telephone number or corresponding sender identification from the order message and stores it for later use as an identifier of the intended recipient of a generated ticket message. At step 403 the application generates the actual ticket message according to some preprogrammed instructions that describe how a ticket message should look like and what should it contain. At step 404 the application inserts the sender identification extracted at step 402 into the message as an identifier of the intended recipient. At step 405 the application takes its own telephone number or corresponding identifier and inserts it into an appropriate sender identification field in the ticket message as a prefix of a complete identifier value. Up to this point the process has executed itself similarly as in prior art electronic ticketing applications.

According to the invention, at step 406 the application reads a code value and inserts it into the sender identification field in the ticket message as a suffix that complements the prefix inserted at step 405 to constitute a complete identifier value. If we assume that the code value is simply some part of the number string that indicates current time, possibly altered with a fixed offset, an advantageous way of executing step 406 is to read current time from a local clock, extract the appropriate numbers from the time value read, refer to a database for finding the currently valid offset value, perform the summing (or other calculational) operation between the extracted numbers and the offset, and write the result into the ticket message under construction. If run-time calculations are to be avoided and/or if the relationship between a time reading and a corresponding code value is more intricate than a pure sum, the database may also include a look-up table prepared beforehand, from which the application finds directly a modified code value by using the local time reading as a key.

At step 407 the application reads once more (if necessary) the local time value and inserts it into an appropriate field in the ticket message as an indicator of original message transmission time. At step 408 the application transmits the completed

ticket message towards an SMSC, typically through a message gateway. Steps 407 and 408 are again similar to corresponding steps known from prior art.

Fig. 5 illustrates the operation of a message gateway functionality according to an embodiment of the invention when it conveys a completed ticket message from a ticket-generating application towards an SMSC. At step 501 the message gateway receives a ticket message from the application, and at step 502 it selects the appropriate SMSC according to certain rules. Typically there is a default SMSC for each subscriber to a mobile telecommunication system and the identity of the SMSC can be derived from the subscribers IMSI (International Mobile Subscription Identifier), fo typically the message gateway reads the recipient identifier at step 502 and uses some simple logic to select the appropriate SMSC. Steps 501 and 502 take place according to practices known from prior art.

At step 503 the message gateway checks, whether the selected SMSC runs CIMD or not. To be more general, we may say that at step 503 message gateway checks, whether the selected SMSC runs a messaging protocol that will only use a possibly transmitted sender's telephone number as a suffix to a preconfigured sender identifier (as in CIMD) or whether the selected SMSC runs a messaging protocol under which it is possible to send a complete sender identifier to the SMSC together with the message. A positive finding at step 503, which means that CIMD or a corresponding protocol is in use, causes a transition to step 504 at which the message gateway deletes the prefix part from the sender identifier that the application has inserted. It is easy to understand that the message gateway need certain unambiguous preprogrammed instructions of how to decide the number of characters to be deleted; assuming our example of always having three characters in the suffix an unambiguous instruction may be as simple as to delete all but the three last characters in a sender identifier string.

A negative finding at step 503 results in a transition to step 505, into which the process also goes after having executed step 504 when needed. Step 505 is a straightforward transmitting step at which the ticket message is transmitted towards the appropriately selected SMSC.

The methods of figs. 4 and 5 do not take any position regarding at which step or device should charging for the ticket be accomplished. Charging is not a matter of interest regarding the present invention, and we may just assume that some known

methods or methods that at the priority date of this patent application are still to be invented are used for charging.

Fig. 6 is a general block diagram of a system 601 according to an embodiment of the invention, in which the message gateway functionality 602 has been integrated into a single system with the ticket-generating application 603. At the disposal of the latter is a database 604, which can be used for various purposes. Closest of these to the present invention is the use of the database 604 as a storage of the currently valid code value. The system includes a web interface 605 through which it is possible to examine and change certain configuration information stored in the database 604. There may also be direct connections for exchanging information between the web interface 605 on one hand and the message gateway functionality 602 and the ticket-generating application 603 on the other hand. As a way of adminstering the database 604 there is a collection of scripts 606, some of which may have been configured to execute automatically at the fulfilment of certain criteria while others must be manually triggered through the web interface 605.

Illustrating all functionalities of fig. 6 in an exemplary way as existing within a single system 601 does not exclude other possible implementations. Parts of the system may be implemented even very far from each other, physically in clearly separate systems, as long as the communication connections between the different functionalities are realised appropriately. For example, it is relatively common that a message gateway functionality exists as a standalone system that serves to selectively connect a number of SMSCs with a number of application servers that run a wide variation of different service applications that utilize messaging.

In the description above we have repeatedly referred to "tickets" and "ticket generation" as an application of the invention. However, the applicability of the invention is not limited to tickets in the sense of admission tickets or travel tickets. The concept of a "ticket" must be understood widely to cover all such instants where a user must or may have at his possession some commodity of value, which ultimately is just a piece of information that proves that the user has committed a certain transaction in a prescribed manner.

We have also mainly described an embodiment of the invention where the code value is derived from the transmission time of the ticket message and inserted into the sender identification (sender's telephone number) field, while the transmission time is inserted into the well-defined transmission time field of the same message.

In principle it is possible to use only the transmission time field for the transmission of both the transmission time and the code value, if the system is allowed to slightly break the conventional rules of handling the transmission time field. An example of this kind is to make the ticket-generating application manipulate the transmission time value so that the minute count and second count would always be the same, or differ from each other by the currently valid offset value, in validly issued ticket messages. Even if a cheater found out that this week the proof of authentication is the fact that the second count is seven more than the minute count in the transmission time value, he would have hard times trying to time the transmission of an illegal copy to his accomplice exactly on the correct second.

Claims

1. A method for authenticating a commodity of value delivered from a closed network as a digital message (201) to a mobile terminal, which digital message (201) has a predefined format that comprises fields (204, 205) for network-generated values (206, 208), **characterized** in that the method comprises the steps of:

- generating (311, 406) a code value according to a time-dependent rule, so that the generated code value depends on the moment of time when the digital message will be transmitted,
- inserting (311, 406) the generated code value into a certain first field (204) in the digital message, which first field has a predefined role that is other than conveying code values, and
- inserting (407) a value that represents message transmission time into a second field (205) in the digital message.

2. A method according to claim 1, **characterized** in that the step of inserting (311, 406) the generated code value into a certain first field (204) in the digital message comprises the substeps of:

- inserting (405) into said first field (204) an identifier (206) of a service for generating and delivering commodities of value, which identifier (206) is smaller in size than a total space available in said first field (204), and
- additionally inserting (311, 406) the generated code value into said first field (204) as a suffix to said identifier (206).

3. A method according to claim 2, **characterized** in that it additionally comprises the steps of:

a) finding out (502, 503), whether the digital message is to be handled according to a first communications protocol that will involve using a preconfigured default identifier in an identifier field of the digital message and adding potentially existing message-contained identifiers after said preconfigured default identifier, and

b) in the case of a positive finding at step a), stripping (504) from said digital message said identifier of a service for generating and delivering commodities of value, before handling said digital message according to said first protocol.

4. A method according to claim 1, **characterized** in that the step of generating (311, 406) a code value according to a time-dependent rule comprises the substeps of:

- obtaining a string of digits that represents a transmission time of the digital message and
- taking a subset of the digits in said string of digits as the code value.

5. A method according to claim 4, **characterized** in that the step of taking a subset of the digits in said string of digits as the code value involves taking a pair of digits that represent a minute count.

6. A method according to claim 4, **characterized** in that the step of taking a subset of the digits in said string of digits as the code value involves taking a pair of digits that represent a second count.

7. A method according to claim 1, **characterized** in that the step of generating (311, 406) a code value according to a time-dependent rule comprises the substeps of:
- obtaining a string of digits that represents a transmission time of the digital message,
- taking a subset of the digits in said string of digits and
- summing a predefined offset value to the number represented by said subset of digits to obtain the code value.

8. An arrangement (601) for generating and delivering authenticated commodities of value that are to be delivered from a closed network as digital messages to mobile terminals, which digital messages have a predefined format (201) that comprises fields (204, 205) for network-generated values (206, 208), **characterized** in that the arrangement comprises:
- means (603, 604) for generating a code value according to a time-dependent rule, so that a generated code value is arranged to depend on the moment of time when a digital message will be transmitted,
- means (603) for inserting a generated code value into a certain first field in a digital message that will be transmitted, which first field has a predefined role that is other than conveying code values, and
- means (603) for inserting a value that represents message transmission time into a second field in a digital message that will be transmitted.

9. An arrangement according to claim 8, **characterized** in that it comprises:
- a commodity-generating application (603) for generating commodities of value and

- coupled to said commodity-generating application (603) a message gateway functionality (602) for delivering generated commodities of value as digital messages to messaging centers for further delivery.

10. An arrangement according to claim 9, **characterized** in that said commodity-generating application (603) is arranged to insert into a first field in generated digital messages an identifier of a service for generating and delivering commodities of value, which identifier is smaller in size than a total space available in said first field, and to additionally insert a generated code value into said first field as a suffix to said identifier.

11. An arrangement according to claim 10, **characterized** in that said message gateway functionality (602) is arranged to:
- find out, whether a digital message that is to be delivered to a certain messaging center is to be handled there according to a first communications protocol that will involve using a preconfigured default identifier in an identifier field of the digital message and adding potentially existing message-contained identifiers after said preconfigured default identifier, and
- strip a part of the contents of an identifier field from digital messages that will be handled according to said first protocol, before delivering such digital messages to messaging centers.

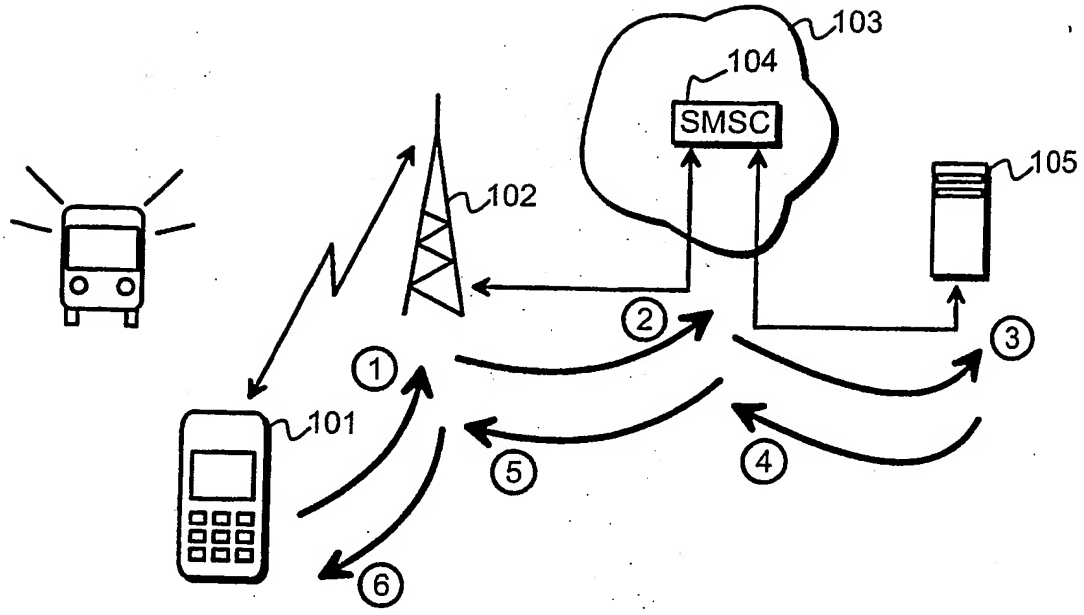

103
104
SMSC
105
102
101
1
2
3
4
5
6

Fig. 1

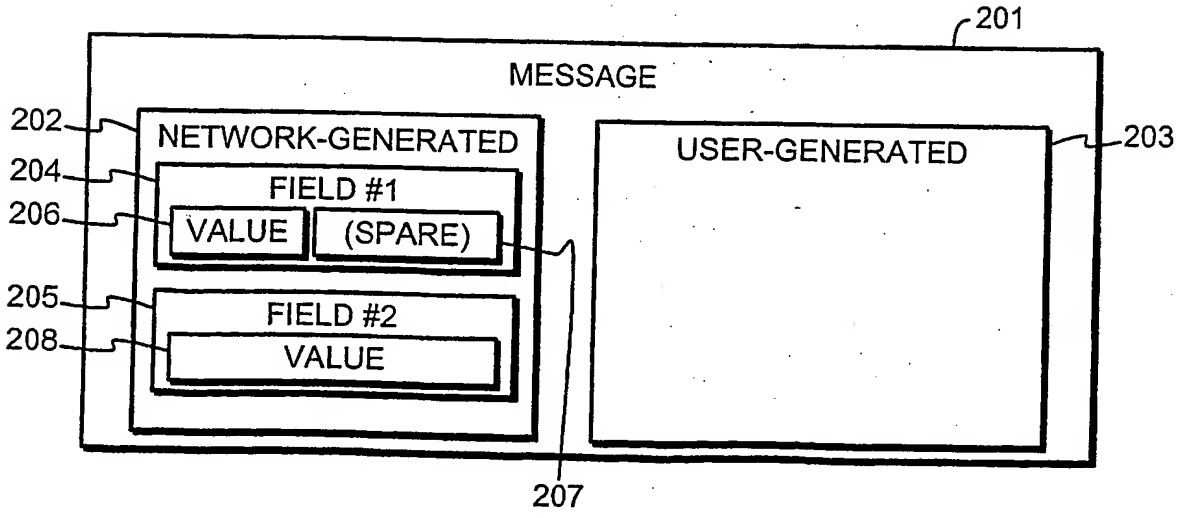

201
MESSAGE
202
NETWORK-GENERATED
204
FIELD #1
206
VALUE
(SPARE)
205
FIELD #2
208
VALUE
USER-GENERATED
203
207

Fig. 2

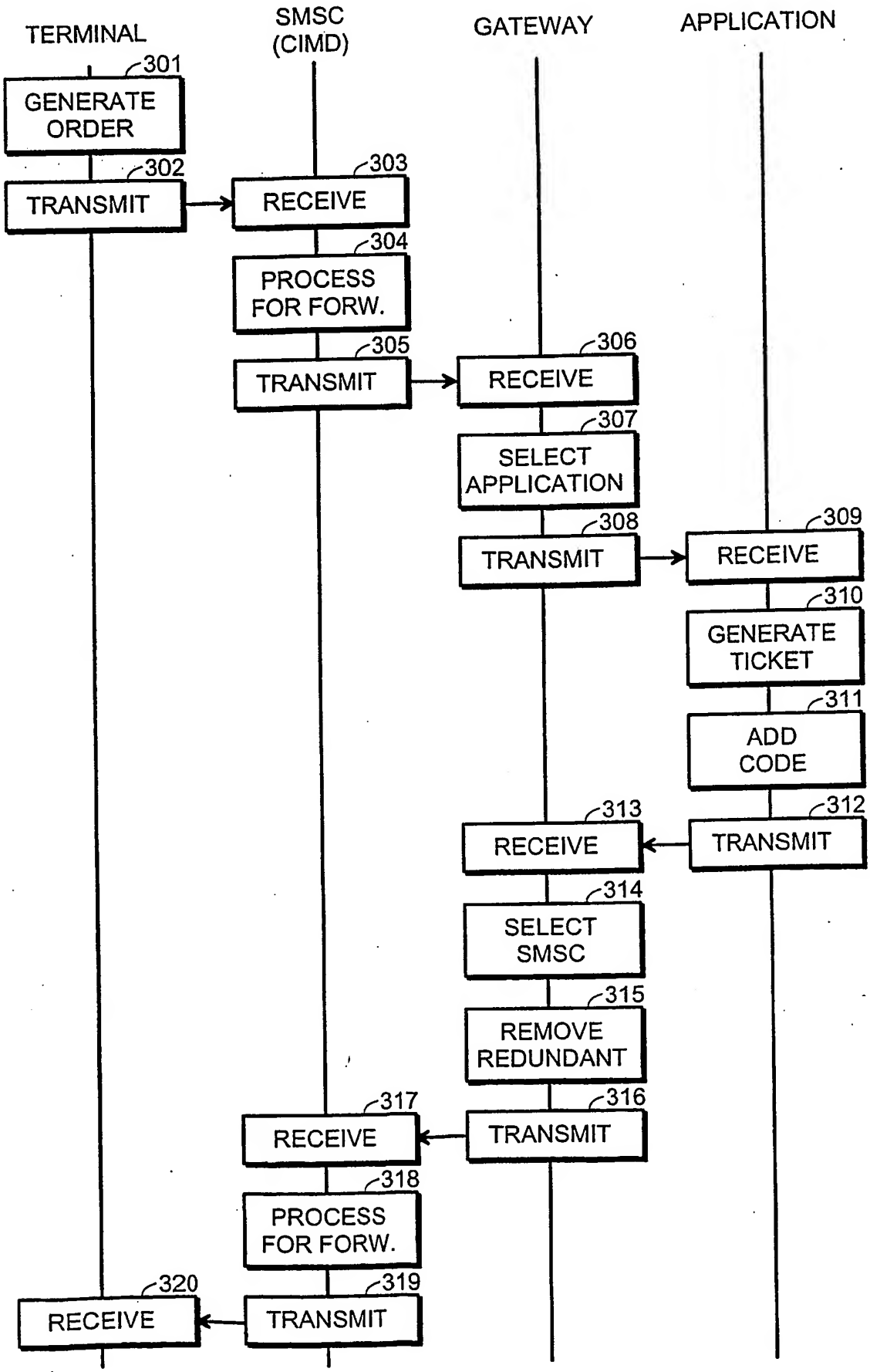

TERMINAL
SMSC (CIMD)
GATEWAY
APPLICATION
301
GENERATE ORDER
302
TRANSMIT
303
RECEIVE
304
PROCESS FOR FORW.
305
TRANSMIT
306
RECEIVE
307
SELECT APPLICATION
308
TRANSMIT
309
RECEIVE
310
GENERATE TICKET
311
ADD CODE
312
TRANSMIT
313
RECEIVE
314
SELECT SMSC
315
REMOVE REDUNDANT
316
TRANSMIT
317
RECEIVE
318
PROCESS FOR FORW.
319
TRANSMIT
320
RECEIVE

Fig. 3a

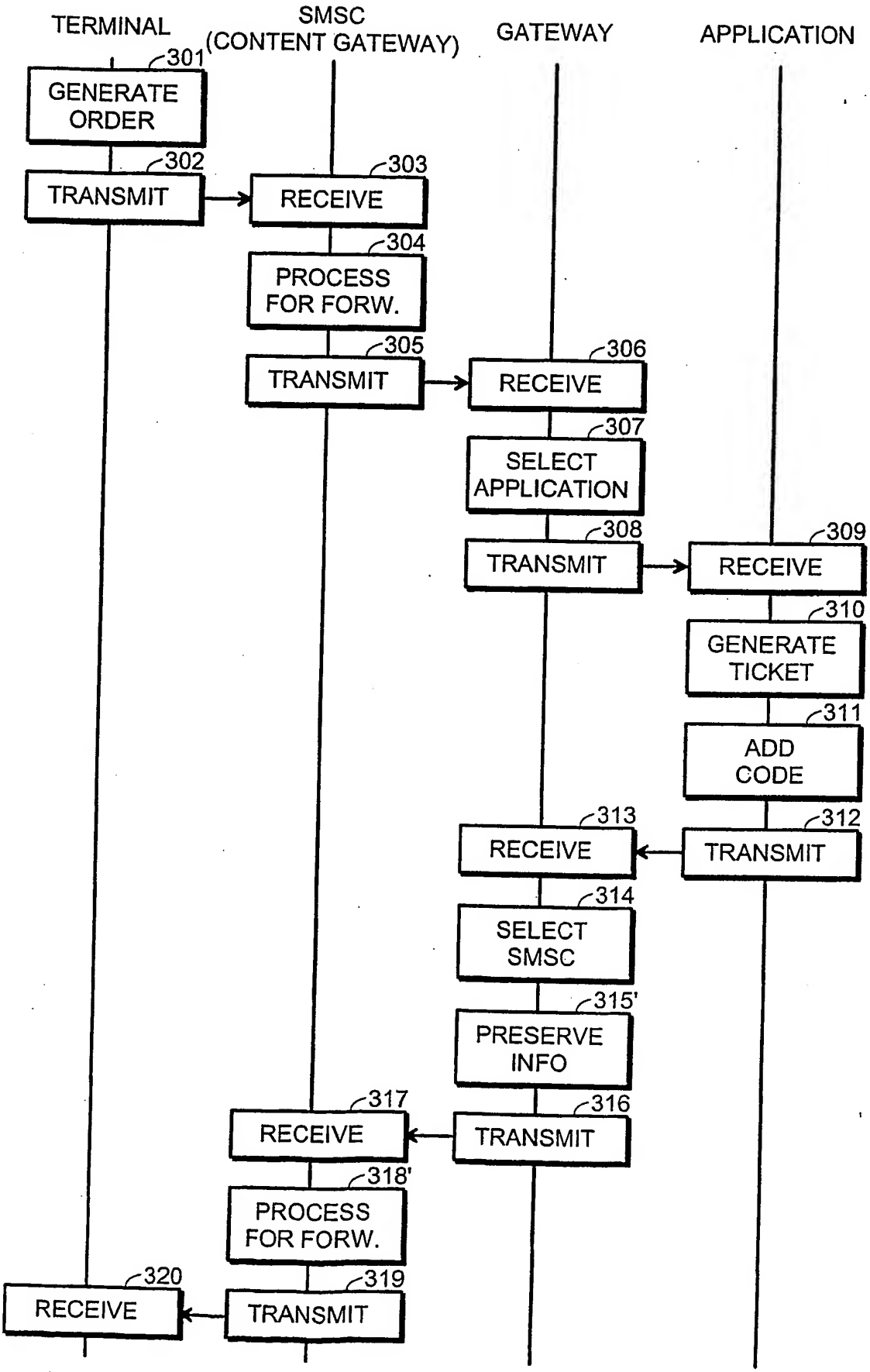

TERMINAL
SMSC (CONTENT GATEWAY)
GATEWAY
APPLICATION
301
GENERATE ORDER
302
TRANSMIT
303
RECEIVE
304
PROCESS FOR FORW.
305
TRANSMIT
306
RECEIVE
307
SELECT APPLICATION
308
TRANSMIT
309
RECEIVE
310
GENERATE TICKET
311
ADD CODE
312
TRANSMIT
313
RECEIVE
314
SELECT SMSC
315'
PRESERVE INFO
316
TRANSMIT
317
RECEIVE
318'
PROCESS FOR FORW.
319
TRANSMIT
320
RECEIVE

Fig. 3b

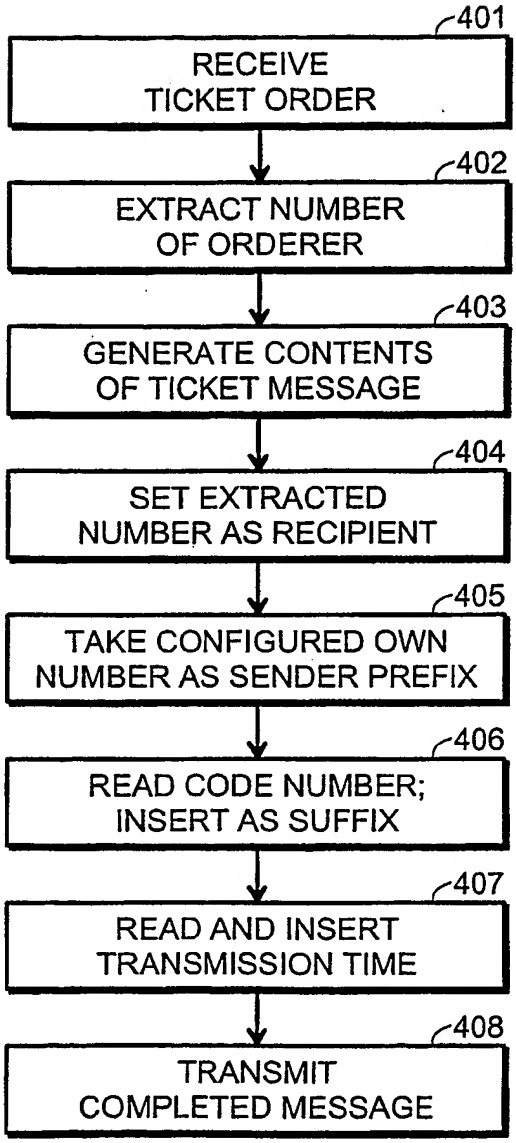

401
RECEIVE TICKET ORDER
402
EXTRACT NUMBER OF ORDERER
403
GENERATE CONTENTS OF TICKET MESSAGE
404
SET EXTRACTED NUMBER AS RECIPIENT
405
TAKE CONFIGURED OWN NUMBER AS SENDER PREFIX
406
READ CODE NUMBER; INSERT AS SUFFIX
407
READ AND INSERT TRANSMISSION TIME
408
TRANSMIT COMPLETED MESSAGE

Fig. 4

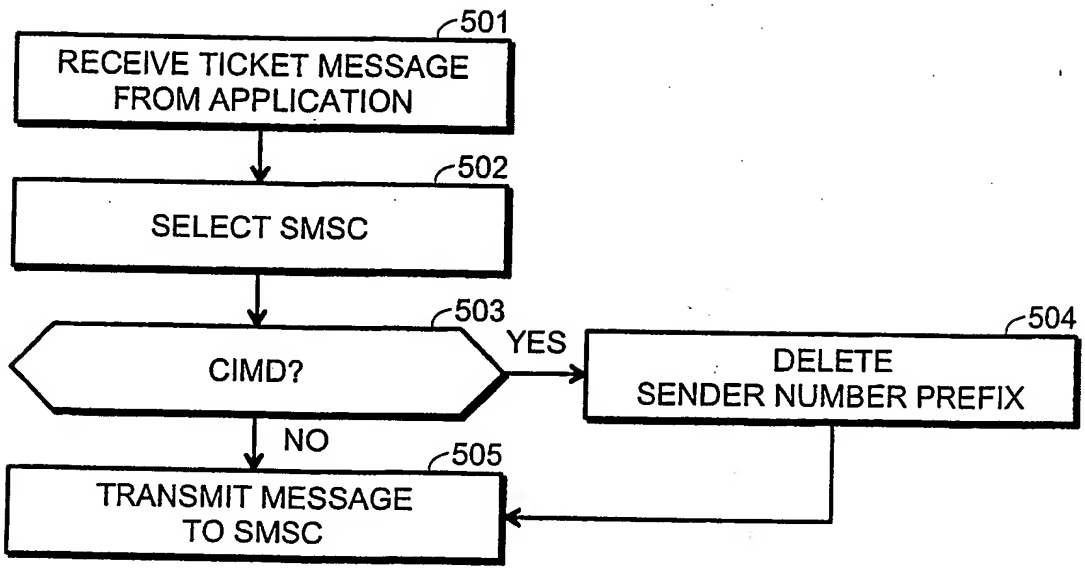

501
RECEIVE TICKET MESSAGE FROM APPLICATION
502
SELECT SMSC
503
CIMD?
YES
504
DELETE SENDER NUMBER PREFIX
NO
505
TRANSMIT MESSAGE TO SMSC

Fig. 5

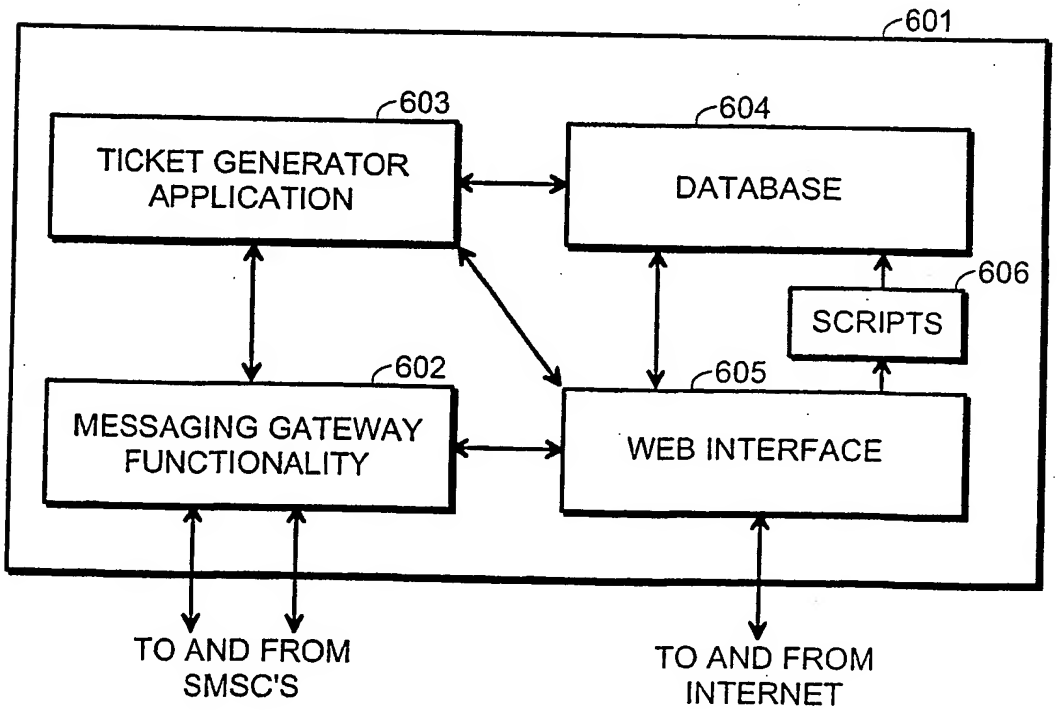

601
603
TICKET GENERATOR APPLICATION
604
DATABASE
606
SCRIPTS
602
MESSAGING GATEWAY FUNCTIONALITY
605
WEB INTERFACE
TO AND FROM SMSC'S
TO AND FROM INTERNET

Fig. 6